REMARKS

Applicant respectfully requests reconsideration of the present application in view of the reasons that follow.

No claims are currently being amended. Claims 1-20 remain pending in this application.

Rejection under 35 U.S.C. § 102

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereafter "Brickell"). Applicant respectfully traverses this rejection for at least the following reasons.

The structure of claim 1 is such that random numbers and a secret key of the owner of a mobile agent are input into a partial signature auxiliary data generation means, and the partial signature auxiliary data generation means generates partial signature auxiliary data based on the random numbers and the secret key of the owner. The generated partial signature auxiliary data is for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts. Brickell fails to suggest at least this feature of claim 1.

Brickell discloses a multi-step digital signature system having a distributed root certifying authority (abstract). The system includes a distributed root certifying authority 20 which includes a set of RCA members 22-30 (Fig. 1, col. 5, lines 36-39). In the signature process of Brickell, an RCE administrator receives a message (which may be a certificate) for signature, and the message is distributed to each of n RCA members (col. 11, lines 18-21). When signing the message, each RCA member separately applies a key fragment to the message without recombining the shares to form a whole key (col. 7, lines 20-22). Each of the RCA members in a key generating group, RCA_{Bi}, selects a random number (x_{Bi}) between 1 and q-1 which is taken to be the private root key fragment for that member (col. 20, lines 22-26).

While Brickell discloses a number of RCAs each signing a message using a different root key fragment, Brickell does not disclose a system including a base host that

generates a partial signature auxiliary data based on a secret key of an owner of a mobile agent, where that partial signature auxiliary data is distributed to remote hosts so that the partial signature auxiliary data will be used when partial signatures that are necessary for calculation of a digital signature of the owner of the mobile agent are calculated by the remote hosts. In the Brickell system, the signed message from one of the RCAs is not generated from a secret key of an owner of a mobile agent and a random number, but each key fragment is individually generated by an RCA member, which is a member of a root certifying authority, as disclosed in column 1, lines 27-28 of Brickell. Thus, Brickell does not anticipate claim 1.

Claim 1 also includes a remote host with a partial signature combining means which outputs a digital signature calculated for signature target data by use of the secret key of the owner of the mobile agent. Brickell also fails to teach this feature of claim 1. Even if the signed messages of the different RCA members are eventually combined, Brickell does not disclose that the messages are combined using a secret key of an owner of the mobile agent. At best Brickell discloses that the signed messages are combined based on contributions from each of the different RCA members, which each have a separate key fragment, but does not disclose that the combination is also based on a secret key of an owner of the mobile agent. Thus claim 1 is further patentable over Brickell for this additional reason.

Moreover, while in the Brickell system fragments of keys are always used in generating a signature in a device (Signing Unit 70), the present invention as claimed allows for input of an encrypted text of the fragments (partial signature auxiliary data) into a remote host when a signature is generated. Consequently, in the invention as claimed, the remote host need not possess a private key for generating a signature, and it becomes easier to control keys. This feature is not suggested by Brickell.

Independent claim 13 includes features similar to, or corresponding to, the features discussed above with respect to claim 1. Namely, claim 13 recites "a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process and a secret key of the owner of the mobile agent as input data and generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts." (emphasis added). Thus claim 13

is patentable over Brickell for reasons analogous to claim 1.

Independent claims 14 and 18 are likewise patentable over Brickell. Claim 14 recites "a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of a secret key of the owner of the mobile agent", while claim 18 recites "a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of the newly generated secret key." Brickell fails to disclose or suggest at least the recited combining process of claims 14 and 18 which is based on a secret key of the owner of the mobile agent, for reasons analogous to those above with respect to claim 1. Thus, claims 14 and 18 are patentable over Brickell.

Independent claims 7 and 17 are likewise patentable over Brickell. Claims 7 and 17 recite "a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means are inputted, which generates a new secret key and a new public key corresponding to the newly generated secret key and generates partial signature auxiliary data for distributing the information of the newly generated secret key to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent" and "a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process as input data, generating a new secret key and a new public key corresponding to the newly generated secret key, generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent". (emphasis added). Brickell fails to disclose at least generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent in the context of claims 7 or 17 for reasons analogous to those above with respect to claim 1.

The Office Action states on page 3 that Brickell describes "[m]essages received at the root certifying authority are distributed to root certifying authority members who attach *partial signatures* to the messages using root key fragments, and enables alteration fragments of private key without need for changing a public key." Even if Brickell describes attaching partial signatures to messages using root key fragments, and alteration of fragments of a private key without need for changing public key, however, Brickell does not disclose use of the private key of the owner of the mobile agent in the same fashion as recited in the claims as discussed above. In this regard, applicant has identified very specific claim limitations in the claims not disclosed by Brickell. If the present rejection based on Brickell is maintained, the Examiner is respectfully requested to specifically point out where Brickell specifically discloses these limitations in the next Office Action.

The dependent claims depend from one of the respective independent claims, and are patentable for at least the same reasons, as well as for further patentable features recited therein.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date May 13, 2005

By Thomas G. Bilodeau

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Thomas G. Bilodeau
Attorney for Applicant
Registration No. 43,438